ICT 2206 – Internet Programming

Individual Project – Fourth Submission

Title: **Design and Implement a Network Infrastructure with VLANs, DHCP Servers, Firewalls, and Internet Connectivity**

Objective:

Design a network for a mid-sized company using Cisco Packet Tracer. The project requires the implementation of VLANs for department separation, DHCP servers for automatic IP assignment, a firewall for network security, and internet connectivity for external communication.

Intended Learning Outcomes:

By completing this project, you will demonstrate skills in VLAN configuration, inter-VLAN routing, dynamic IP address assignment, firewall setup, and basic internet connectivity for an enterprise network.

Scenario:

You are a network administrator for a company that has *n* user departments, *m* administrative departments, *p* academic departments, and 1 security and emergency response department. Each department must be assigned to its own VLAN for logical separation and security. The company also requires dynamic IP address assignment using DHCP, with a single DHCP server with VLAN interfaces for the internal networks.

You must configure a firewall to secure the network and allow selective internet access. Additionally, three computers should be allocated for guest access in each user department so that visitors can access the services the relevant department provides. These three computers should be allocated the last three statically allocated IP addresses in each department. These computers are only allowed to access the services available in the department (no access to the Internet or outside the respective VLAN).

PCs in the administrative departments should be able to access all PCs in user departments except the PCs allocated for guest access. However, PCs in one

administrative department should be denied access to other administrative departments (if any) or the emergency response department.

Network Requirements:

1. **Departments (VLANs)**:
    - Each VLAN should be assigned numbers in the range of 10, 20, 30, …
    - Each VLAN should be assigned separate /24 address ranges.
2. **Devices**:
    - Each VLAN should be serviced with a separate Layer 2 switch
    - 1 Router (Layer 3, configured as a gateway and firewall)
    - 1 Internet Cloud (Simulated internet access)
    - 1 DHCP server with VLAN interfaces
    - At least 3 PCs for each department
    - Additional 3 PCs for each department with static IP addresses
3. **DHCP Configuration**:
    - For each VLAN, the upper half of the allocated addresses should be provided through DHCP
4. **Firewall**:
    - Permit internet access for all VLANs.
    - Block external access to internal networks.
    - Block the newly added PCs from accessing outside their VLANs.
    - Allow PCs in the management networks to access PCs in the user departments
    - Block PCs in the management networks from accessing PCs allocated for guest access in user departments.
    - Block PCs in one management network from accessing other management networks or the emergency response department.
5. **Internet Connectivity**:
    - Connect the router to an ISP via the internet cloud (use simulated connectivity).

Changes in the Scenario for the Fourth Submission:

PCs in the emergency response department should be able to access all PCs in user, management, and academic departments. However, PCs outside the

emergency response department should be denied access to the emergency response department. Further, a separate internet connection is provided for the academic and emergency response departments.

Network Requirements:

1. **Departments (VLANs)**:
    - No change.
2. **Devices**:
    - 1 Router (Layer 3, configured as a gateway and firewall)
    - 1 Internet Cloud (Simulated internet access)
3. **DHCP Configuration**:
    - No change.
4. **Firewall**:
    - Allow PCs in the emergency response network to access all PCs in the other departments
    - Block PCs in other networks from accessing PCs in the emergency response network.
    - Allow all traffic to and from the internet from academic and emergency response networks only through the new internet connection.
5. **Internet Connectivity**:
    - Connect the new router to a different ISP via the internet cloud (use simulated connectivity).

Tasks to Complete for Submission 04:

1. **Network Topology Design**:
    - No change.
2. **VLAN Configuration**:
    - No change.
3. **Router Configuration**:
    - Set up static routing or default routing in the new router to the simulated internet.
4. **DHCP Server Setup**:
    - No change.
5. **Firewall Configuration**:

- Allow PCs in the emergency response network to access all PCs in the other departments
- Block PCs in other networks from accessing PCs in the emergency response network.
- Allow all traffic to and from the internet from academic and emergency response networks through the new internet connection.
- Deny traffic to and from the internet from academic and emergency response networks through the old internet connection

6. **Internet Connectivity**:
   - Configure internet access through the new router using a default route pointing to the internet cloud.
   - Test connectivity from the PCs in academic and emergency response networks to ensure they can access the web.
7. **Testing and Verification**:
   - Ensure that PCs in the emergency response department can communicate with PCs in the user departments and vice versa is not allowed.
8. **Documentation**:
   - Document all configurations (commands) for the new router and the firewall and the complete set of firewall rules.

Submission Requirements:

- Packet Tracer Project File (.pkt)
- Text file containing the configurations (commands) for the new router and the firewall and the complete set of firewall rules

---